UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,026	08/27/2001	Lane W. Lee	M-12041 US	4898

7590 10/18/2005

Theodore P Lopez
MACPHERSON KWOK CHEN & HEID LLP
1762 Technology Drive
Suite 226
San Jose, CA 95110

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/940,026	LEE ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-14,16-18 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-14,16-18 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the Request for Continued Examination (RCE) filed on July 29, 2005. Claims 1-2, 5-14, 16-18, and 20 are currently being considered.

Response to Arguments

2. Applicant's arguments with respect to claims 1-2, 5-14, 16-18 and 20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 20 is rejected under 35 U.S.C. 102(e) as being anticipated by Hurtado et al. (U.S. Publication No. 2003/0105718).

Regarding claim 20, Hurtado discloses:

A storage engine configured to certify a host, the engine comprising:

a firmware component including:

a block configured to receive a certificate from the host, the certificate including a plurality of fields, including a field holding a protocol public key (Figures 1 – 6, paragraphs 205 – 213);

a block configured to verify one or more digital signatures in the certificate including at least one of:

a certifying authority digital signature using a certifying authority public key (Figures 1 – 6, paragraphs 205 – 209); and

a device digital signature using a device public key in the certificate (Figure 1 – 6, paragraphs 303 – 324); and

a block configured to receive validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria (Figures 1 – 6, paragraph 181, paragraph 185, paragraphs 206 – 215);

a block configured to transmit a session key to the host when the digital signatures are verified and validated (Figures 1 – 6, paragraph 18, paragraph 181, paragraph 185, paragraphs 206 – 215); and

a block to transmit an encrypted content key to the host, wherein the host enabled to recover a content key from the encrypted content key by using the session key (Figures 1 – 6, paragraph 18, paragraph 181, paragraph 185, paragraphs 206 –

215), wherein the end user key is used to decrypt the secure container containing the decrypting key (content key) used to decrypt the content.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 5-14, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hurtado et al. (U.S. Publication No. 2003/0105718) in view of Liu et al. (U.S. Patent 6,760,752).

Regarding claim 1, Hurtado discloses:

A method of authenticating a host to receive content from a storage engine, the method comprising:

receiving at the storage engine a certificate from the host, the certificate including a plurality of fields, including a field holding a digital signature from a certifying authority (Figures 1 – 6, paragraphs 205 – 213);

verifying the digital signatures in the certificate, the verifying including at least one of:

verifying the certifying authority digital signature using the certifying authority public key (Figures 1 – 6, paragraphs 205 – 209); and

verifying a host digital signature using a device public key (Figure 1 – 6, paragraphs 303 – 324); and

receiving validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria (Figures 1 – 6, paragraph 181, paragraph 185, paragraphs 206 – 215); and

if the digital signatures are verified and validated, generating a random number at the storage engine and encrypting the random number with a public key extracted from the certificate to form a session key and transmitting the session key to the host (Figures 1 – 6, paragraph 18, paragraph 181, paragraph 185, paragraphs 206 – 215);

at the host, receiving an encrypted content key from the storage engine (paragraph 18, , paragraph 181, paragraph 185, paragraphs 206 – 215), wherein the decrypting key in the secure container is used to decrypt the content; and

decrypting the encrypted content key using the session key to recover the content key (paragraph 18), wherein the end user key is used to decrypt the secure container containing the decrypting key (content key) used to decrypt the content.

Hurtado does not explicitly disclose "if the digital signatures are verified and validated, generating a random number at the storage engine and encrypting the random number with a public key extracted from the certificate to form a session key and transmitting the session key to the host." Liu discloses a secure transmission system wherein the encrypting step can include "generating a random number,

encrypting the message using the random number as a session key in a symmetric key encryption algorithm and encrypting the session key using a public key encryption algorithm and the public key of the recipient" (column 2 lines 33-37). Hurtado and Liu are analogous arts as both disclose a method of sending a secure message by encrypting the message (secure container) with a session key (end user encrypting key). Hurtado discloses that a secure container containing a decrypting key (content key) is encrypted with a end user key (session key) and transmitted to the recipient. Liu extends this idea by establishing how the session key is formed (by generating a random number) and encrypted (by a public key). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method of forming the session key (by a random number) and encrypting it using a public key, in order to "ensure the integrity of information sent over the Internet" (column 1 lines 30-33) as stated by Liu.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein the source is one of a portable medium and firmware (Figure 1 – 6, paragraph 181, paragraph 185, paragraphs 206 – 215).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein the certifying of the host includes certifying a second host for a host to second host secure communication channel, certifying allowing a copy function between the host and the second host (paragraph 246 – 249).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein the data in the certificate specifies one or more of a product category, a product line, a model, a revision and a serial number of the host (paragraph 457).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein the certificate includes one or more of a certifying authority identifier field, a version field, a sign key identifier field, an exposed methods field, a company field, a model identifier field, a revision field, a metadata identifier field, a device digital signature key field, a certifying authority digital signature field, a serial number field, a protocol public key field and a device digital signature field, wherein the certifying authority digital signature verifies one or more of the fields in the certificate and the host digital signature verifies one or more of the fields in the certificate (paragraph 229, 251, 293).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein the certificate enables an entity receiving the certificate to control the quality of the host by invalidating devices that are false or have latent defects (Figures 6 – 10, paragraph 457).

Claim 13 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein the certificate specifies one or more certificate classes, the certificate classes providing a set of methods that may be exposed after the transmitting the session key (paragraphs 880 – 884).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein each of the fields holds 326-bit values for 163-bit elliptic curve cryptography (paragraph 52, paragraphs 193-197, paragraphs 248-256).

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein the certifying authority public key is referenced by a field of the certificate (pages 18 – 23).

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Hurtado discloses:

The method of claim 1 wherein the certifying authority public key is in a firmware component (Figures 1 – 6, paragraph 181, paragraph 185, paragraphs 206 – 215).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Hurtado discloses:

The method of claim 6 wherein the source validation data is compared with the data in the certificate to identify as invalid one or more of the product category, the product line, the model, the revision and the serial number of the host (paragraphs 462 – 463).

Claim 10 is rejected as applied above in rejecting claim 6. Furthermore, Hurtado discloses:

The method of claim 6 wherein the certificate further includes fields provided by a host manufacturer, including the company public key, wherein the company public key is digitally signed by the certifying authority (pages 18 – 23).

Claim 11 is rejected as applied above in rejecting claim 6. Furthermore, Hurtado discloses:

The method of claim 6 wherein the certificate further includes fields provided by a host manufacturer, the fields including the device public key, wherein the host public key is digitally signed by the company (pages 18 – 23).

Claim 12 is rejected as applied above in rejecting claim 6. Furthermore, Hurtado discloses:

The method of claim 6 wherein one or more of the product category, the product line, the model, the revision and the serial number of the host are provided to a certificate creator after the host passes a qualification procedure (paragraph 457).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Hurtado discloses:

The method of claim 13 wherein the set of methods includes digital rights management (DRM) methods include one or more of a copy method, a record method, a play method, a read secure metadata method, a write secure metadata method, and an unlock method, the DRM methods operable according to a type of the host (paragraph 10).

Regarding claim 20, Hurtado discloses:

A storage engine configured to certify a host, the engine comprising:

a firmware component including:

a block configured to receive a certificate from the host, the certificate including a plurality of fields, including a field holding a protocol public key (Figures 1 – 6, paragraphs 205 – 213);

a block configured to verify one or more digital signatures in the certificate including at least one of:

a certifying authority digital signature using a certifying authority public key (Figures 1 – 6, paragraphs 205 – 209); and

a device digital signature using a device public key in the certificate (Figure 1 – 6, paragraphs 303 – 324); and

a block configured to receive validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria (Figures 1 – 6, paragraph 181, paragraph 185, paragraphs 206 – 215);

a block configured to transmit a session key to the host when the digital signatures are verified and validated (Figures 1 – 6, paragraph 18, paragraph 181, paragraph 185, paragraphs 206 – 215); and

a block to transmit an encrypted content key to the host, wherein the host enabled to recover a content key from the encrypted content key by using the session key (Figures 1 – 6, paragraph 18, paragraph 181, paragraph 185, paragraphs 206 – 215).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
10/14/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100